

WHAT IS CLAIMED IS:

1. A computer-implementable method of performing modulo division, using a dividend N and an n-bit divisor D to produce a remainder R, said method comprising:
when $D=2^n-1$ and $0 \leq N \leq (D-1)^2$, non-iteratively processing $N \bmod D$ to produce the remainder R

2. A computer-implementable method of performing modulo division, using a dividend N and an n-bit divisor D to produce a remainder R, said method comprising:
when $D=2^n-1$ and $0 \leq N \leq (D-1)^2$, performing $N \bmod D$ to produce the remainder R,
where a number of processing operations necessary to produce the remainder R is

5 independent of n.

3. A computer-implementable method of performing modulo division, using a dividend N and an n-bit divisor D to produce a remainder R, said method comprising:

when $D=2^n-1$ and $0 \leq N \leq (D-1)^2$, summing the upper $\lceil \frac{n}{2} \rceil$ and lower $\lfloor \frac{n}{2} \rfloor$ bits of the

dividend N to produce the remainder R.

4. The computer-implementable method of claim 1, further comprising the step of subtracting the divisor D from the sum to produce the remainder R, if the sum is greater than the divisor D.

5. The computer-implementable method of claim 2, further comprising the step of subtracting the divisor D from the sum to produce the remainder R, if the sum is greater than the divisor D.

6. The computer-implementable method of claim 3, further comprising the step of subtracting the divisor D from the sum to produce the remainder R, if the sum is greater than the divisor D.

7. The computer-implementable method of claim 1, wherein $n \geq 2$.

8. The computer-implementable method of claim 3, wherein $n \geq 2$.

¹⁵
9. The computer-implementable method of claim ¹³~~3~~, wherein $n \geq 2$.

³
10. The computer-implementable method of claim ²~~7~~, wherein $n \geq 3$.

⁹
11. The computer-implementable method of claim 8, wherein $n \geq 3$.

¹⁶
12. The computer-implementable method of claim ¹⁵~~9~~, wherein $n \geq 3$.

¹⁸
13. An apparatus for performing modulo division, using a dividend N and an n-bit divisor D to produce a remainder R, said apparatus non-iteratively processing $N \bmod D$ to produce the remainder R, when $D=2^n-1$ and $0 \leq N \leq (D-1)^2$.

²⁵
14. An apparatus for performing modulo division, using a dividend N and an n-bit divisor D to produce a remainder R, said apparatus performing $N \bmod D$ to produce the remainder R, where a number of processing operations necessary to produce the remainder R is independent of n, when $D=2^n-1$ and $0 \leq N \leq (D-1)^2$.

³²
15. An apparatus for performing modulo division, using a dividend N and an n-bit divisor D to produce a remainder R, said apparatus summing the upper $\lceil \frac{n}{2} \rceil$ and lower $\lfloor \frac{n}{2} \rfloor$ bits of the dividend N to produce the remainder R, when $D=2^n-1$ and $0 \leq N \leq (D-1)^2$.

³³
16. The apparatus of claim 13, said apparatus subtracting the divisor D from the sum to produce the remainder R, if the sum is greater than the divisor D.

17. The apparatus of claim 14, said apparatus subtracting the divisor D from the sum to produce the remainder R, if the sum is greater than the divisor D.

³³
18. The apparatus of claim ³²~~15~~, said apparatus subtracting the divisor D from the sum to produce the remainder R, if the sum is greater than the divisor D.

¹⁸
19. The apparatus of claim ¹³~~13~~, wherein $n \geq 2$.

²⁶
20. The apparatus of claim ²⁵~~14~~, wherein $n \geq 2$.

³⁴
21. The apparatus of claim ~~18~~³², wherein $n \geq 2$.

²⁰
22. The apparatus of claim 19, wherein $n \geq 3$.

²⁷
23. The apparatus of claim ~~20~~²⁶, wherein $n \geq 3$.

³⁵
24. The apparatus of claim ~~21~~³⁴, wherein $n \geq 3$.

²⁸
25. The apparatus of claim ~~14~~²⁵, wherein said apparatus is a component of a Reed-Solomon coder.

³⁰
26. The apparatus of claim ~~15~~³², wherein said apparatus is a component of a Reed-Solomon coder.

<sup>Swi
ad</sup>
27. The apparatus of claim ~~16~~, wherein said apparatus is a component of a Reed-Solomon coder.

³⁸
28. A computer program embodied in a computer readable medium for performing modulo division, using a dividend N and an n-bit divisor D to produce a remainder R, comprising:

a summing code segment for summing the upper $\lceil \frac{n}{2} \rceil$ and lower $\lfloor \frac{n}{2} \rfloor$ bits of the

5 dividend N to produce the remainder R, when $D = 2^n - 1$ and $0 \leq N \leq (D-1)^2$.

³⁹
29. The computer program of claim ~~28~~³⁸, further comprising a subtracting code segment for subtracting the divisor D from the sum to produce the remainder R, if the sum is greater than the divisor D.

⁴⁰
30. The computer program of claim ~~28~~³⁸, wherein $n \geq 2$.

⁴¹
31. The computer program of claim ~~30~~⁴⁰, wherein $n \geq 3$.

⁴²
32. A computer signal for performing modulo division, using a dividend N and an n-bit divisor D to produce a remainder R, said computer signal comprising:

T 0120
T 0131

a summing code segment for summing the upper $\lceil \frac{n}{2} \rceil$ and lower $\lfloor \frac{n}{2} \rfloor$ bits of the dividend N to produce the remainder R, when $D=2^n-1$ and $0 \leq N \leq (D-1)^2$.

⁴³
~~33~~. The computer signal of claim ⁴²~~32~~, further comprising a subtracting code segment for subtracting the divisor D from the sum to produce the remainder R, if the sum is greater than the divisor D.

⁴⁴
~~34~~. The computer signal of claim ⁴²~~32~~, wherein $n \geq 2$.

⁴⁵
~~35~~. The computer signal of claim ⁴⁴~~34~~, wherein $n \geq 3$.

~~add~~
~~as~~

09324644 0833393